PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-237632
(43)Date of publication of application : 13.09.1996

---

(51)Int.Cl.
H04N 7/167
H04H 1/00
H04K 1/00
H04N 7/16

---

(21)Application number : 07-294880
(22)Date of filing : 18.10.1995
(71)Applicant : GENERAL INSTR CORP OF DELAWARE
(72)Inventor : EYER MARK
SHUMATE ALLEN
MORONEY PAUL

---

(30)Priority
Priority number : 94 324591 Priority date : 18.10.1994 Priority country : US

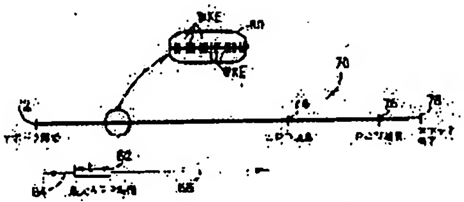
---

(54) METHOD AND DEVICE FOR FREE PREVIEW OF COMMUNICATION NETWORK SERVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a time-limited preview of a program to be purchased through a communication network in a cryptographically secure manner any virtual time during the service of the preview.

SOLUTION: The proposed method has specific applicability to the provision of video services on a pay-per-view basis. The video service is provided during the period of a program epoch(PE). When portions of the video service are available for viewing by a preview system, fixed time 72-74 is formed in the PE 72-78. A customer can previously view portions of the video service any time during the period of fixed time within maximum preview time 82 shorter than fixed time 72-78 without purchasing the service. After previously viewing portions of the video service, the customer can purchase the video service during the period of a program epoch 72-78. Plural records are stored so that the service of different previewable programs can be simultaneously received.



LEGAL STATUS
[Date of request for examination] 15.03.1996
[Date of sending the examiner's decision of rejection] 10.11.1998
[Kind of final disposal of application other than

Disclaimer:
This English translation is produced by machine translation and may contain errors. The JPO, the NCIPI, and those who drafted this document in the original language are not responsible for the result of the translation.

Notes:
1. Untranslatable words are replaced with asterisks (****).
2. Texts in the figures are not translated and shown as it is.

Translated: 01:15:02 JST 11/09/2006
Dictionary: Last updated 09/29/2006 / Priority: 1. Electronic engineering / 2. Mechanical engineering / 3. JIS (Japan Industrial Standards) term

---

FULL CONTENTS

[Claim(s)]

[Claim 1] When the process which is a method for providing video service to a consumer through an information network, and provides meter-rate based video service in program epoch, and said a part of video service can be seen beforehand, He has no purchase in said a part of video service always before the short-time maximum preview epoch time and during said fixed time than the process which forms fixed time in said program epoch, and said fixed time. How to consist of the process beforehand shown to a consumer and the process which strengthens said maximum preview epoch time with the security method by encryption.

[Claim 2] How to be a method according to claim 1 and consist of the process at which a consumer can purchase said video service for seeing in said program epoch after showing the part beforehand further.

[Claim 3] The method which is a method according to claim 1 or 2, and said program epoch is divided into two or more working key epoch (WKE), and consists of the process which attests said calculation of WKE by encryption, and the process which uses this attested calculation and gives said maximum preview time further.

[Claim 4] From Claim 1, to either of 3, are the method of a description and During said fixed period, The method that consist of the process holding the record which can direct the amount of the intact preview time which remains to said consumer who looks at said video service further, and said record is held by the security method by encryption.

[Claim 5] The process holding record of the service which is a method given in either of 4 from Claim 1, and said consumer has seen beforehand in former program epoch, How to consist of the process which forbids said consumer from looking at service beforehand into the present program epoch when said consumer has seen all the portions of this service beforehand in former program epoch further.

[Claim 6] The method that are a method according to claim 5 and said record of service is held

by the security method by encryption [Claim 7] It is a method given in either of 6 from Claim 1, and is a process holding the AKUCHIBU record to N of the service which can be previewed at a certain time. The record of purchase as which each of this record expresses the service which was purchased by said consumer, and which can be previewed, Or the method of consisting of the process which consists of either of the preview records as which said consumer expresses the service chosen between previews, and the process which does not make the service record in which an AKUCHIBU preview is possible complete until the program epoch for the service expressed by the record is completed further.
[Claim 8] How to consist of the process which does not eliminate any preview records further until the service which is a method according to claim 7 and is expressed by it is completed.
[Claim 9] How to be a method according to claim 7 and consist of the process prevented from changing the record of purchase which acquired preview record from the process changed into record of purchase by purchase by the consumer of service to whom it is expressed by this preview record, and said process to change further.
[Claim 10] How to consist [is a method according to claim 9, and] of the process which does not eliminate any preview records further until the program epoch for the service expressed by it is completed except for being based on conversion to the record of purchase which cannot be changed.
[Claim 11] It is the method of consisting of the process which refuses any previews to said consumer further always, when it is a method given in either of 10 from Claim 7 and all the service records that can preview N pieces are AKUCHIBU.
[Claim 12] How to be a method given in either of 11, and include further the process which the amount of intact preview time tells to said consumer that it is which remains in said video service from Claim 1.
[Claim 13] The method that are a method given in either of 12 from Claim 7, and said fixed time is strengthened with the security method by encryption.
[Claim 14] It is equipment for offering the preview of the service which can be purchased through a communication network. It is the 1st means for processing the data which receives from said communication network. said data identifies the service in which (1) purchase is possible -- (2) -- [the epoch for which said service is provided / identify and] (3) 1st means to offer information required to generate a key to be able to indicate whether a preview is available with said service, and for the consumer by whom (4) permissions were done receive said service or its preview, If what it is 2nd means to answer said 1st means, and is seen beforehand is permitted when a preview is available with said service 2nd means to hold the truck of fixed time between said epoch, They are said 1st and 2nd means and the user interface which has two incomes so that a consumer can see said a part of service beforehand before the short-time maximum preview time and during said fixed time rather than said fixed

time at any time. [with said user interface / a consumer] the user interface which can also purchase said service, during a preview, and after the purchase Equipment which consists of a means to answer said 1st means for decoding said service.
[Claim 15] Equipment which is equipment according to claim 14 and consists of the means for strengthening said maximum preview time with the security method by encryption further.
[Claim 16] Equipment which consists of the means for holding record by the security method by encryption further in order to direct the amount of the intact preview time which is equipment given in Claim 14 or either of 15, and was left behind to said consumer who can see said service during said fixed time.
[Claim 17] It is equipment given in either of 16 from Claim 14, and is a means for holding record to N of the service in which an AKUCHIBU preview is possible at a certain time. The record of purchase as which each of this record expresses the service which was purchased by said consumer, and which can be previewed, Or until the program epoch for a means and the service expressed by the record which consists of either showing the service chosen for the preview of said consumer of the preview records is completed Equipment which consists of the means for not making the service record in which an AKUCHIBU preview is possible complete further.
[Claim 18] Equipment which is equipment according to claim 17, and consists of the means for not eliminating any preview records further until the program epoch for the service expressed by it is completed.
[Claim 19] [are equipment according to claim 17 and / preview record / purchase by the consumer of service to whom it is expressed by this preview record] Equipment which consists of the means for changing into record of purchase, and the means for the ability not to change the record of purchase offered by the means for [said] changing further.
[Claim 20] Equipment which is equipment according to claim 19, and consists of the means for not eliminating any preview records further until the program epoch for the service expressed by it is completed except for being based on conversion to the record of purchase which cannot be changed.
[Claim 21] It is equipment which consists of the means for also refusing the service in which what kind of additional preview or additional preview is possible to said consumer always when it is equipment given in either of 20 from Claim 17 and all the service records that can preview N pieces are AKUCHIBU further.
[Claim 22] Equipment which consists of the means for telling said consumer about the amount of the intact preview time which is equipment of a description and remains in Claim 14 or either of 21 with said service further.
[Claim 23] Equipment which it is equipment given in Claim 14 or either of 22, and said epoch is divided into two or more working key epoch, and is used in order that the calculation attested

by the encryption may give said maximum preview time.
[Claim 24] Equipment with which it is equipment given in Claim 14 or either of 23, and a preview consists of a means for attesting the portion of said data by encryption at least to identify whether it is available, further with said service.
[Claim 25] Equipment with which it is equipment given in Claim 14 or either of 24, and said fixed period is strengthened with the security method by encryption.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the cable TV which can receive service for pay, satellite TV, and a communication network like computer network. Before purchasing the offer work of each program (for example, film program) especially, it is related with the method and equipment for offering the free preview (free preview) of this offer work.
[0002]
[Description of the Prior Art] The cable TV and satellite TV which can receive video service for pay are known well. Moreover, the comp serve (CompuServe), pro DEJI (Prodigy), Other things of the charge which can access America Online, dialog (Dialogue) data utility, a database and banking (banking), and shopping service, and can perform communication of an E-mail etc. are known. Some communication networks have provided service by the free trial system (free trial basis) conventionally. For example, the meter-rate based telefilm which a televiewer orders the film which pays and looks at a charge can sometimes show a televiewer first about 5 minutes of the film of a preview system (preview basis), before purchase is required. Such a preview was restricted between the predetermined time at the time of the start of a film. The free preview has never obtained during broadcast of a film.
[0003] To be able to supply the restricted free preview may be desired by the consumer in any time under broadcast of service (for example, film). It must have been forced so that it may be a televiewer at the start time of a program, he may accept it with video service and it may have a preview, and it may be time inconvenient to a televiewer. However, in any time while service has come to hand, it is filled for supply of the free-with the time limit preview at danger, considering the position of a service provider. Especially the thing for which service is opened to a free preview always can make it possible for all the services to come to hand, without a lawless televiewer's or lawless "Pirates's" destroying SEKYURITEI of a signal, and paying a charge.
[0004] It may be an advantage during supply of service to offer the method and equipment for following a free-with the time limit preview in any imagination time. Furthermore, it may be an

advantage to offer a method and equipment which do not bring an outlaw or Pirates a profit easily. Such a method and equipment should maintain signal SEKYURITEI, giving the pliability of "a full time free preview (Anytime free preview, AFP)." Moreover, it may be an advantage to offer the method and equipment which a televiewer can change between one or more AFP(s) (each relates to separate service) and in an ordinary program. Each AFP may be restricted to the specific maximum AFP time of itself. Security of such a system must always be carried out, and it must prevent a televiewer getting the free preview beyond the maximum time prepared in specific service. This invention offers the method and equipment which have the advantage mentioned above and other advantages.

[0005]

[Means for solving problem] The method of this invention provides video service to a consumer through an information network. Video service is provided by the meter-rate system in program epoch (program epoch). When a part of video service can see by a preview system, fixed time (fixed period) is formed in program epoch. A consumer can see a part of video service without purchase beforehand by the short-time maximum preview time rather than fixed time during this fixed time at any time. This maximum preview time (maximum preview dulation) is suitably strengthened with the security method (cryptographically secure manner) by encryption. In particular, record is held by the security method by encryption, it points to the amount of the intact preview time left behind to the consumer, and video service can be seen during fixed time. Like the data which identifies whether a preview can receive specific service for a part of video service during this fixed time, it can see beforehand and fixed time is also suitably held by the security method by encryption.

[0006] In the suitable example, the method of this invention can purchase video service for a consumer to see in program epoch after looking at a part of service beforehand. Moreover, this program epoch is divided into two or more working key epoch (WKE) in the suitable example. The calculation of WKE is attested by encryption. This attested calculation is used in order to give the above-mentioned maximum preview time (that is, the truck of this maximum preview time is formed and held).

[0007] This method consists of the process holding record of the service which the consumer looked at beforehand in former program epoch further. This consumer is right, and when all the portions of that service have been seen in former program epoch, he forbids pre viewing of service in the present program epoch. This prevents that a consumer records a continuous free preview, in order to accumulate all of the film for seeing, or other programs. Record of the service which the consumer looked at beforehand in former program epoch is held by the security method by encryption.

[0008] In the example of a graphic display, the AKUCHIBU record to N of the service which can be previewed is held simultaneously. Each record consists of either showing the service chosen for the preview of the record of purchase showing the service which was purchased by the consumer, and which can be previewed, or a consumer of the preview records. It is barred until the program epoch for the service as which expiration of the service record which can be previewed by AKUCHIBU is expressed by the record is completed. Expiration time is controlled by an expiration timer. Expiration is barred in modification by establishing the fixed minimum record time (for example, several hours) to each record. The fixed minimum record time is longer than the longest service which has an available free preview.

[0009] The method of this invention does not eliminate any preview records until the program epoch for the service expressed by it is completed. In the example of a graphic display, preview record is changed into record of purchase by purchase by the consumer of service to whom it is expressed by preview record. It becomes impossible to change record of purchase simultaneously with change. In such the example, blanking of which preview record is barred until the program epoch for the service expressed by it is completed except for preview record being eliminated by change to the record of purchase which cannot be changed.

[0010] When all of N records of the service which can be previewed are AKUCHIBU, an additional preview is refused to a consumer always. However, the consumer can still purchase service, one of the preview records overlaps record of purchase, and it is written here. Suitably, the preview record ended next overlaps and is written. If preview record is opened wide, the amount of the intact preview time which remains in corresponding video service will be told to a consumer.

[0011] The equipment of this invention offers the preview of the service which can be purchased through a communication network. The 1st means processes the data which received from the communication network. This data identifies the service in which (1) purchase is possible, and a time [to provide (2) services (epoch)] period is identified. (3) Offer information required for that of ****** for a key to point to whether a preview is available with service, and for the consumer by whom (4) attestation was done receive service or its preview. If pre viewing is permitted, 2nd means to answer the 1st means when a preview is available with service will be established in order to hold the truck of fixed time in epoch. The 1st and 2nd means for a consumer to see a part of service beforehand in any time in fixed time till the short-time maximum preview time and a user interface have two incomes rather than fixed time. With this user interface, a consumer can also purchase service. During a preview and after the purchase, a means to answer the 1st means for decoding service is.

[0012] The equipment of this invention consists of the means for strengthening the maximum preview time with the security method by encryption further. This equipment holds record by the security method by encryption, and directs the amount of the intact preview time which remains in the consumer who can see service during fixed time.

[0013] The means for holding simultaneously the AKUCHIBU record to N of the service which can be previewed is established. Each record consists of either showing the service chosen for the preview of the record of purchase showing the service which was purchased by the consumer, and which can be previewed, or a consumer of the preview records. A means by which the service record which can preview AKUCHIBU is not made to complete is established until the program epoch for the service expressed by the record is completed. Furthermore, the means for not carrying out blanking of any preview records is established until the program epoch for the service expressed by that cause is completed. In the example of a graphic display, the means for changing preview record into record of purchase is established by purchase by the consumer of service to whom it is expressed by preview record. The record of purchase given by this change means cannot be changed. It is barred until the program epoch for the service as which blanking of which preview record is expressed by it except for the possible change to the record of purchase which cannot be changed is completed.

[0014] The equipment of this invention consists of the means for refusing the service in which what kind of preview or preview is possible further to a consumer always, when all of the service records which can preview N pieces are AKUCHIBU. Moreover, the means for telling a consumer about the amount of the intact preview time which remains in each service is established.

[0015] The epoch for which service is provided is divided into two or more working key epoch in the example of a graphic display. The calculation attested by encryption of working key epoch is used in order to give the above-mentioned maximum preview time. The means for attesting further at least one of the data with which fixed time while the preview is previewing [whether it is available and] by identifying with the above-mentioned service is permitted by encryption is established.

[0016]

[Mode for carrying out the invention] Drawing 1 is the block diagram of decipherment portions, such as a satellite of a digital type, or a cable TV receiver. The enciphered service (for example, premium television service (Premium television service)) is inputted into a terminal 10. The bit stream which consists of service is inputted into a terminal 10, and is sent over a communication channel using indigenous technology, and from this communication channel, it already receives and is modulated. The enciphered service is decoded by the decipherment processor 12, it is the output 16 of this decipherment processor, and a pure signal is given.

[0017] a decipherment processor -- an ordinary decipherment scheme -- for example, U.S. Pat. No. 4613901 of gill-box HAUZEN (Gilhousen) and others (Title of invention: the signal encryption and the distributed system (Signal Encryption) for controlling the alternative remote desk run bull and scramble of a TV signal) and Distribution System for Controlling Scrammbling U.S. Pat. No. 4864615 of andSelective Remote Descrambling of Television Signals, or Bennett (Bennett) and others (Title of invention: [the distributed key generation data]) What is indicated by reproduction (Reproduct of Secure keys By Using Distributed Key Generation Data) of the security key by using it is used. A decipherment processor needs a working key (WK), in order to decode the signal inputted there through a terminal 10. A working key answers the control signal received through input/output (I/O) terminal 30, and is generated by the protection processor 20. The firmware used for a protection processor is stored in ROM24. A protection processor is prepared with RAM22 by ordinary specification again. The protection part of RAM22 holds the module specification key for using it by the monthly key (monthly key), and/or seed (seed), as shown in drawing 2 .

[0018] The user interface 26 can make a televiewer choose the service for seeing on television (TV) 28. If it is attested in order that a user may receive the service chosen by subscription or each purchase (for example, meter-rate system), [the protection processor 20] A switch 18 is moved and the decoded output 16 is connected to TV28 through a user interface 26 from the decipherment processor 12. In other words, a user interface and TV only receive the enciphered signal through a line 14 and a switch 18.

[0019] The class of a typical key is shown in drawing 2 . The enciphered program Puri key (program pre-key) is inputted into the decipherment function 44 through a terminal 40, and it receives monthly key (monthly key) through a terminal 42 again. The program Puri key is different from each enciphered program work (for example, TV program), and applicable to a decipherment. A monthly key is changed once periodically every month, for example. The decipherment function 44 decodes the enciphered program Puri key, gives a program Puri key, and is used as one input of the one-way function 48. The input of others to the one-way function 48 consists of various program attributes (the requirements for access are included) used for a corresponding column. This requirement for access must agree, in order to acquire attestation and to watch a program. It is inputted through a terminal 46, a one-way function processes a program Puri key and a program attribute, and a program attribute gives a program key. The program key outputted from the one-way function 48 is used as one input to other one-way functions 52 which receive the initialization vector (IV) expressed with time through a terminal 50. Processing of the program key by the one-way function 52 and an initialization vector decodes the service which generated the working key required of the decipherment processor 12 (drawing 1), and was chosen by the attested user. Other various description of formation of a key containing a working key (given by a "key stream") is known by patent of above-mentioned Bennett and others.

[0020] Drawing 3 is a diagram of an initialization vector inputted into the terminal 50 of the one-way function 52. The initialization vector 60 is started by time =I, to time =J, several weeks, Laon (run) is carried out and calculation is reset, for example. Two or more program epoch (from PE1 to PEn) occurs during the time expressed with a vector 60. Each program epoch is different length and relates to one program work.

[0021] Drawing 4 is the diagram of one program epoch expressed with a sign 70. It starts in time 72 and epoch is ended in time 78. Before termination of epoch, the AFP boundary 74 and the program boundary 76 are. The time between a start and the AFP boundary 74 of epoch 72 is the fixed time in program epoch, when it can use in order for a part of program to see by a preview system. A program can be previewed during the maximum AFP time 82 during this fixed time. Although it can see also in which time from the start of epoch to an AFP boundary, AFP is till the given maximum AFP time "t", as the arrows 84 and 86 of drawing 4 show. The maximum AFP time 82 is maintained as a working key, and it decreases so that permissible AFP time may be used up, so that it can change again, in order for a televiewer to be able to see some portions of the free preview time permitted, or to see the remaining portion.

[0022] A working key is generated among program epoch for the attested member who had purchased or applied for the preview of the program during preview time. This program epoch is divided into two or more working key epoch (WKE) 80 as shown in drawing 4 . For example, working key epoch is generated at intervals of desirable others in the rate of per second eight WKE(s), or the thing given to the system. WKE gives the convenient means for maintaining accumulation of the AFP boundary 74. In the suitable example, an AFP boundary is the value of WKE showing this boundary, and a full time (anytime) free preview is not permitted across this boundary. This parameter is attested by including it in a program key generation machine. A maintenance and study of an AFP boundary are hereafter explained in detail in relation to drawing 6 and 7.

[0023] The program boundary 76 is the point which the program sponsored in epoch will end. Termination of epoch 78 is extended across the program boundary 78, and becomes the possibility of the program continued covering the length from the first expected. For example, if a program is interrupted by the news flash, the termination time of a program can extend. Since similarly it is impossible to predict termination of a game of a sport correctly, a program boundary is extended within program epoch and it can respond to the game which rushes in at excess time.

[0024] According to this invention, a free preview is not permitted at all after an AFP boundary. Therefore, a free preview is not obtained between [some] the programs between the AFP boundary 74 and the termination 78 of epoch. The Reason for preparing an AFP boundary is for the defense to trespass of Pirates who is going to get a program or service for nothing using AFP. In order to obtain free service, especially Pirates can try to change the termination time of program epoch. However, this is the value with which the AFP boundary was attested, and since it cannot obtain a free preview more than this value, it does not help to wrest a continuous full time free preview. Furthermore, this invention establishes "record" of the program previewed and purchased, and these records are not immediately completed by a method which is assistance [Pirates] so that it may explain in detail below.

[0025] In order to prevent capture of service with the advantage of a full time free preview, the protection processor 20 (drawing 1) of this invention specifies certainly the period of the program segment which can be seen without purchasing. In order to attain this, the period of a full time free preview is held at the module of working key epoch. The protection processor 20 carries out calculation of the number of the generated free working key. this calculation -- a maximum of -- if the limit established by the AFP time 82 (drawing 4) is reached, an attestation state will be changed by "only purchase is possible" from "it is possible to purchase or obtain a free preview." This AFP time is one of the program attributes included in formation of a program key. Therefore, alternation must have been carried out for not carrying out the alternation of the program key itself, and the right decipherment of a program is protected.
[0026] or [as mentioned above, / having seen the system of this invention beforehand] -- or record of each purchased program is established. In order that a user may look at AFP, once it chooses, "preview record" is made from the protection processor 20, the number of the free working key permitted is formed, and since record is completed when an event or a program is completed, a real time counter will be maintained. The timer must continue carrying out Laon of whether a receiver is compounded by scramble or the enciphered wave, and, thereby, record completes it at effective time. If AFP record expires at an early stage, the 2nd free viewing time will be taken. If this record expires late, although it is harmless, the number of a new free preview work decreases, while record is after termination of a program.
[0027] According to this invention, the multiplex function record up to N pieces is held. Each record is either "preview record" showing the full time free preview chosen by the user, the "record of purchase" showing the program purchased by the user or non-AKUCHIBU (NARU (null)) record. Moreover, it is impossible to eliminate, before an event is completed if an event or the lawful purchase of the service in which other purchase is possible is removed according to this invention to preview record of the given event, and in such a case, record overlaps, is written and gives record of purchase. A user decides typically whether to charge a free preview, next to purchase the event based on this free preview. If an event is not purchased, preview record is held till termination of an event, unless other services are purchased, it overlaps and it is written. Preview record will be changed into record of purchase if a user decides to purchase an event.
[0028] The process which does not make preview record eliminate before an event is completed is the indispensable feature of this invention. If preview record is only saved in a first-in first-out (FIFO) train and new record will be added, old record can disappear. Then, it returns in order for beyond free preview restrictions to see repeatedly, next to see other free previews of a desired program by scanning and seeing between a small portion of number of a program in order that a user may clarify a train. This opportunity will once be beforehand eliminated by each maintenance of preview record of all events, if preview record is

established.

[0029] Moreover, according to this invention, priority is given to the purchase of a program over a free preview work. All of N available preview/records of purchase are AKUCHIBU, and when at least one record holds AFP, the protection processor 20 directs the attestation state "purchase is possible." This is because one of preview record is taken and replaced with record of purchase, even if all of available preview/records of purchase are used. The preview record taken and replaced with record of purchase is the closest to expiration suitably.

[0030] For a user, it is also important to control any opportunities carefully, and since the capability to eliminate preview record gives the opportunity of misuse, preview record is eliminated. For example, the program "purchased" has been made as Pirates considers. Therefore, when program purchase (for example, record of purchase) overlaps and writes preview record, this invention offers various defense. A user's decoder is increased for the purchase which overlaps and writes preview record to the 1st by the cost of a program here including the debtor's (debit) security transfer. Calculation of the number of purchase is carried out by the method of security again. The record of purchase itself remains in memory storage till termination of the purchased event the 2nd. In this way, the record cannot perform procurement of other full time free previews till termination of the purchased event.

[0031] When the program chosen for purchase is a program formed by preview record, the record is only changed into record of purchase, and it is left with the record opening wide. After preview record is made into AKUCHIBU, purchase next to the program cannot be canceled. Record of a program is not eliminated in this way. Furthermore, the protection processor 20 establishes the last expiration time of record of purchase. This minimum time is the order of 1 hour, and frustrates the potential trespass by Pirates who record of purchase is made to complete at an early stage, and tries as like, for example.

[0032] The timing of a full time free preview and a program period is held by the protection processor 20. A real time program expiration counter is held at a protection processor for this purpose. A program period and AFP time are given to the module of working key epoch.

[0033] As mentioned above, record of 1 set of multiplex functions is held at the protection processor 20, and treats the program purchased [which purchased and full-time-free-previewed]. 1 set of N a preview / program records are shown in drawing 5 in diagram. Record 90, 92, 94, 96, and 98 include the specific event or the program attribute (the requirements for access are included) of a program to which record is related, respectively. a maximum of [for preview record to look at a free preview] -- AFP time -- there is nothing -- the calculation (for example, number of the free working key which remains) of the time which remains is also held. When record of purchase is established after a free preview, it becomes impossible to cancel.

[0034] The requirements for access for which a user has to apply in order that a program attribute may receive the cost of a program, and a program [obtain / (for example, "an old thing (tiers)") and AFP / a program] [give / for AFP / supposing it is sleeve **** / the free working key of which] It consists of the free preview boundary of the first stage in the case of a first stage free preview receiving instead of a full time free preview, or being added to a full time free preview, and information like various local access information. Since the requirements for access are attested by the one-way function 48 as shown in drawing 2 , it does not carry out by turns, without carrying out the program key used in order for all these requirements to generate the working key for decoding a program by turns. In order to decode, when it differs from what is used for encryption of the program key used, a decipherment goes wrong. as the requirements for access -- a maximum of -- inclusion of AFP time (for example, the permission was granted free number of WK) protects what was carried out by turns [that], without attesting this parameter and repealing a working key.

[0035] Each preview/record of purchase contain a part of a record effective flag, purchase flag, expiration timer calculation, and program key used as a program discrimination circuit. A record effective flag is a 1-bit flag, and directs whether record is effective, for example. If this flag is set up, it directs that the contents of record are effective. When this flag is clearance (clear), record is not formed now.

[0036] A purchase flag directs that record explains record of purchase instead of preview record. A setup of a purchase flag will carry out the insect of the working key epoch calculation. Calculation of the expiration timer is carried out in the module (for example, 2.56 seconds) in which time passed in the program and which was formed beforehand. Expiration of record will once clear a record effective flag.

[0037] A part of program key given to a preview/record of purchase consists, for example of 5 bytes of clearance program key, and it is used as a program discrimination circuit. Working key epoch calculation carries out calculation of the number of the working key given during a full time free preview.

[0038] As a part of guidance of an attestation state required as the ability of a user to watch a program, a protection processor is determined, when the given program can see through a full time free preview. Even if all of N available preview/records of purchase are using it (it is directed with a record effective flag like), a free preview cannot be received when provided for the program of specification [AFP].

[0039] Such operation is not suitable although preview record is established at each time which a user adjusts to the channel which offers AFP. This is because the program which offers AFP encounters continuously and N available records are used up, shortly after a user adjusts continuously to another program. [therefore, the user interface 26 (drawing 1)] [probably provide the user with the option so that AFP can see, when available, and] the case for which directions of the amount of the free preview time which remains in the program are given to a user and which will come out and exist where it carries out and an early free preview (a program -- offer a preview during [which was restricted] the first portion very much) and a full time free preview work are mutually related further is treated -- I will come out. In the suitable example, a user interface is given through the screen display top on a user's television 28. The formation on such a screen display is common knowledge in the conventional technology.

[0040] Generally, the screen display is available, when a protection processor opts for an available thing in the program which AFP acquired. A user interface collects the text messages which form an AFP option screen. If a user chooses AFP, a user interface tells the protection processor 20 about this thing, and free access can be received by maximum AFP time. In the modification example, when sufficient time passes after the user adjusted in specific service, AFP can receive automatically.

[0041] In order to treat the possible collision between an early free preview and a full time free preview, being reinforced with various rules is suitable. It should be disregarded that AFP is offered when a program is acquired [1st] during an early free preview (or between previous epoch). a program with user same to the time after a user chooses not purchasing a program and an early free preview is completed -- encountering (that is, it returning to the program, after adjusting to a thing different from the program) -- AFP may be offered. The program purchased during AFP time by the 2nd is not canceled. If purchase is made during AFP time, this purchase is the present thing and it cannot once change.

[0042] Drawing 6 and 7 are the flow charts illustrating processing of the full time free preview given according to this invention. A routine is started with a box 100 and the message of working key epoch is obtained with a box 102. A WKE message identifies WKE calculation within the present program epoch. The message of a program Puri key is obtained with a box 104. As shown in drawing 2 , a program Puri key is needed in order to generate the working key and program key for the attested user. When the user is attested with the ability of all AFP (s) given for the program and the program to be received with the box 106, in order to determine, the attestation state for a user is calculated. If attested with the ability of a user to receive a program, determination will be made with a box 108 like whether it pointed to the program which a user wants to purchase. If that is right, record of purchase will be made with a box 110. By making record of purchase, a portion with an imperfect clearance (outputted from one-way function 48 of drawing 2) program key is saved with a box 112. This clearance program key is used by the one-way function 52 (drawing 2), and draws a required working key as shown with a box 114.

[0043] Although a working key is generated, determination is made with a box 116 about whether program epoch was completed. If it has not ended, it is continued, and processing will carry out the loop of the guidance of a working key until program epoch is completed between a box 114 and 116. After program epoch is completed, it is eliminated as record of purchase shows with a box 118. This routine is ended with a box 120 next.

[0044] When the program has not been purchased yet by the attested user, a routine is performed from a box 108 to a box 122, and the determination about whether program epoch was completed is made here. If it has ended, a routine will be ended with a box 120. Determination is made about whether a program is [procurement of a full time free preview] able not to be completed if it becomes. If that is not right, a routine will return to a box 108.

[0045] when AFP is available in a program (for example, AFP calculation without zero -- as [show / or / by the separated AFP available bit]), determination is made with a box 126 about whether it requires, in order that a user may look at a free preview. If AFP is required, a routine will go to the box 128 of drawing 7 . Preview record is made with a box 128. Next, an AFP expiration counter (AEC) is initialized with a box 130. With a box 132, a clearance program key is saved with AFP calculation. AFP calculation decreases with each working key, and gives record (that is, amount of the time left behind to watching a free program by the televiewer) of the time which remains in maximum AFP time.

[0046] With a box 134, a working key is made and AFP calculation decreases. Next, program expiration time is directly calculated from the present working key epoch, as a box 136 shows. Expiration of AFP record with this way is dynamically calculated again by each working key. Variable M is calculated in particular. Here, it is M= (AFP boundary - the present WKE calculation). Next, M is changed at real time using easy scaling, and when larger than AEC as which this result was determined with the box 138, it is a box 140, and AEC overlaps the calculated expiration time and is written. In order to extinguish preview record and to obtain additional AFP of a program, this prevents Pirates from it shortening AEC, and extends AEC to a sake. AEC is tested, and if required, after being overlapped and written, determination will be made with a box 146 about whether AFP maximum time was extended (that is, when the number of the free working key of a preview has decreased to zero). If that is right, no attesting any further things of AFP of a program will be supposed with a box 152. Moreover, determination is made about whether it passed through the AFP boundary with a box 146. An AFP boundary is the working key epoch calculation showing that boundary, and a full time free preview is not permitted across this boundary. As mentioned above, this parameter is attested at a program key generation term including it.

[0047] Passage of an AFP boundary will presuppose no attesting any further things of AFP of a program with a box 152. Moreover, determination is made about whether AFP was ended by the user with a box 148. If that is not right, as for a routine, waiting and a working key new subsequently will be made with a box 134 in the following working key epoch (box 149). Next, a routine is continued until AFP maximum time expires, until it passes through an AFP boundary, or until AFP is ended by the user. By the termination of AFP by a user, the present number of AFP hour meters is performed until a program is purchased, until program epoch is completed, or until AFP is required again. It can make him initialize a full time free preview again in front of an AFP boundary and in a program until maximum AFP time completes the number of AFP hour meters to a user.

[0048] Drawing 6 and the routine of 7 return to a box 108 by-less attesting AFP, after holding the number of AFP hour meters after AFP's is ended by the user, or maximum AFP time expires or passing through an AFP boundary. Next, if program epoch is not completed, a user can purchase a program or service.

[0049] In the modification example, calculation of the expiration time (the box 130 of drawing 7 , and 136-140) from WKE and the maintenance of an AFP expiration counter are eliminated by only setting up the minimum preview record expiration time. For example, the once established preview record is maintained for the 2 minimum hours. This cannot protect full time free preview characteristics, and Pirates cannot wrest one or more AFP(s) for ** 2 hours. It is used, in order to protect expiration of the service record which can be AKUCHIBU previewed until the program epoch of the service as which the method shown in this method or drawing 7 is expressed by that record is completed when the minimum preview record expiration time is longer than the longest typical program epoch.

[0050] What should be understood here is that this invention offers a free preview for the meter-rate based service on a communication network. As an enticement which can purchase service, the potential program purchase machine (program purchaser) which can be seen with the time limit of a film or other programs is given. This invention improves the conventional technology which only the portion of the beginning of a film can see for free. It has the full time free preview of this invention, and the preview is not restricted to the portion of the beginning of service. The period of a free preview is variable and can be formed on a program by a program system by specifying as a program attribute or maximum AFP time. In this invention, once a user looks at an available free preview, in order to see the additional portion of this free preview, it can return again. The user cannot disunite a free preview in the portion of many [having wished], and cannot exceed maximum AFP time at this time.

[0051] Although this invention was explained in relation to the specific example, probably, it turns out that various modification objects and change objects proper-do to a person skilled in the art, without deviating from the soul and the range of this invention of a description to Claims.

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is the block diagram of the equipment of this invention.

[0052]

[Drawing 2] Drawing 2 is the block diagram showing the class of the decipherment used according to this invention.

[0053]

[Drawing 3] Drawing 3 is a time line and shows different program epoch generated over time.

[0054]

[Drawing 4] Drawing 4 is the diagram of one program video image, and shows various boundaries included there and the sample of the working key epoch (WKE) which happens into program epoch.

[0055]

[Drawing 5] Drawing 5 is the diagram of record of various previews/programs which are maintained according to this invention.

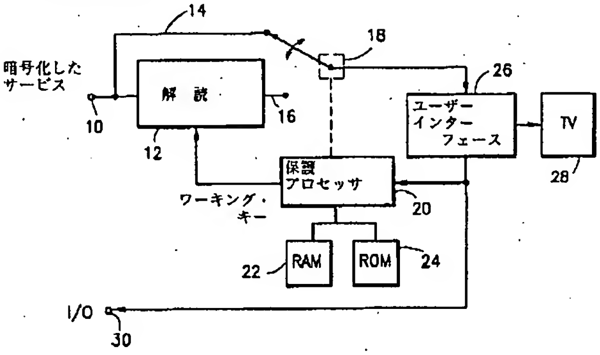
[0056]

[Drawing 6] Drawing 6 is the portion of the beginning of the flow chart which shows attestation of a full time free preview according to this invention.

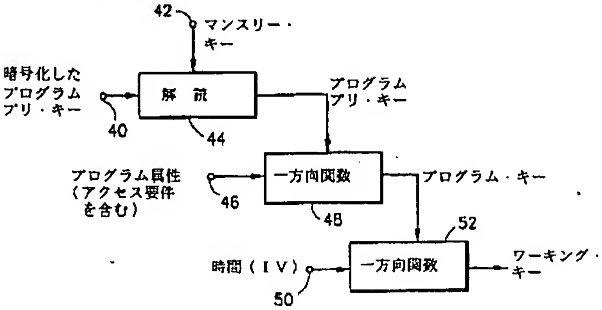
[0057]

[Drawing 7] Drawing 7 is the portion of a continuation of the flow chart of drawing 6 .

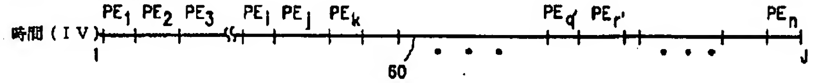
[Drawing 1]


14
18
暗号化した
サービス
解読
16
26
10
12
ユーザー
インター
フェース
TV
28
保護
プロセッサ
ワーキング・
キー
20
22
RAM
ROM
24
I/O
30

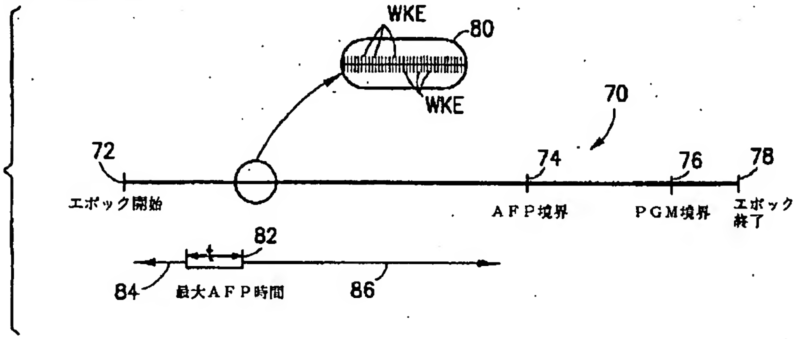
[Drawing 2]


42
マンスリー・
キー
暗号化した
プログラム
プリ・キー
解読
プログラム
プリ・キー
40
44
プログラム属性
（アクセス要件
を含む）
46
一方向関数
プログラム・キー
48
52
時間（ＩＶ）
一方向関数
ワーキング・
キー
50

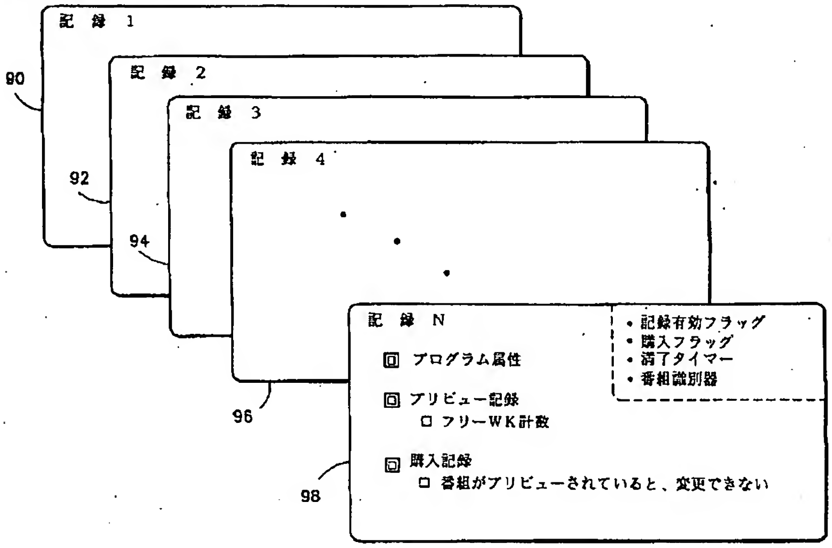
[Drawing 3]


時間（IV）
PE$_1$
PE$_2$
PE$_3$
PE$_i$
PE$_j$
PE$_k$
PE$_q$
PE$_r$
PE$_n$
I
J
60

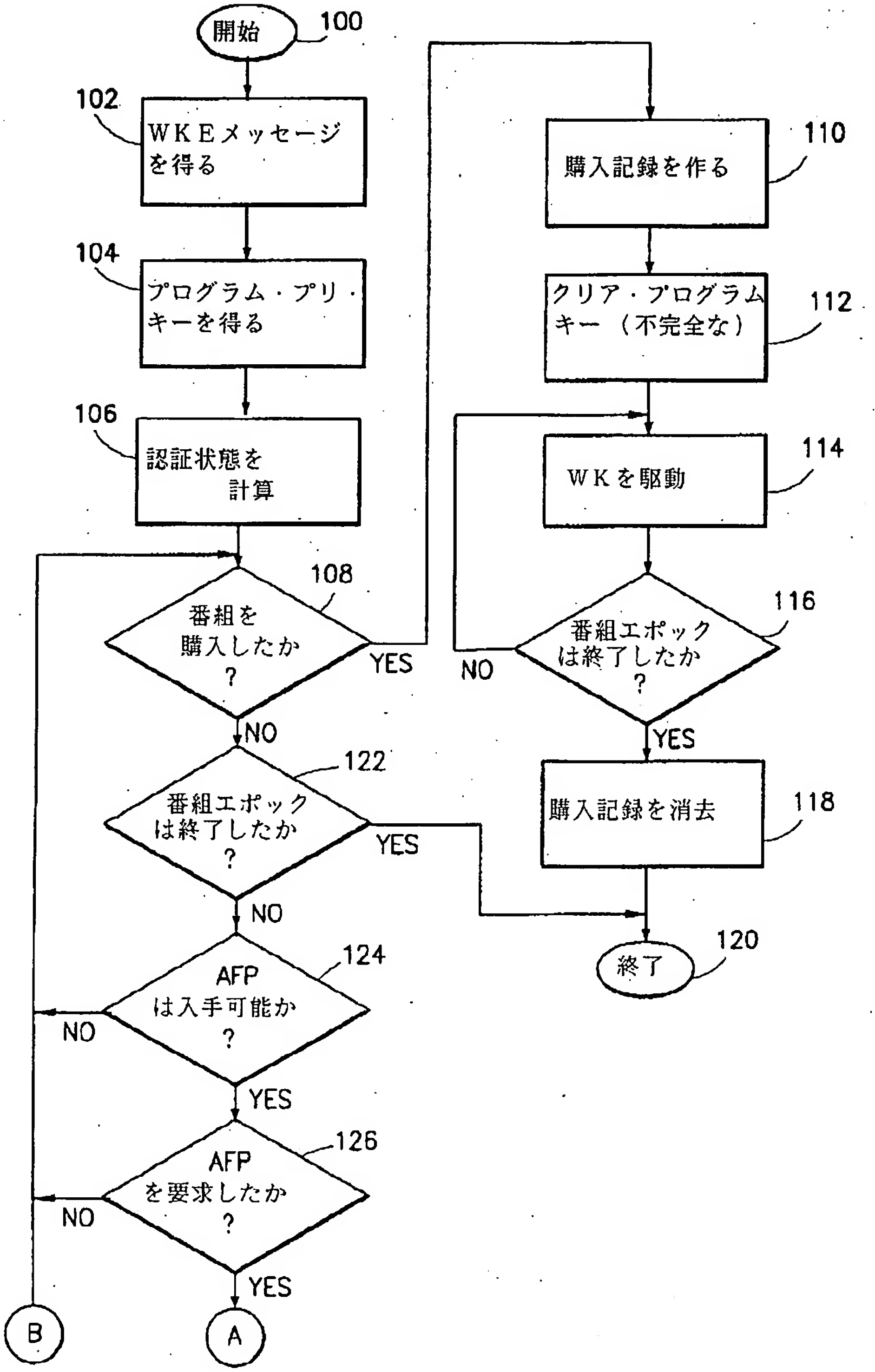
[Drawing 4]


WKE
80
WKE
70
72
74
76
78
エポック開始
AFP境界
PGM境界
エポック終了
82
t
84
最大AFP時間
86

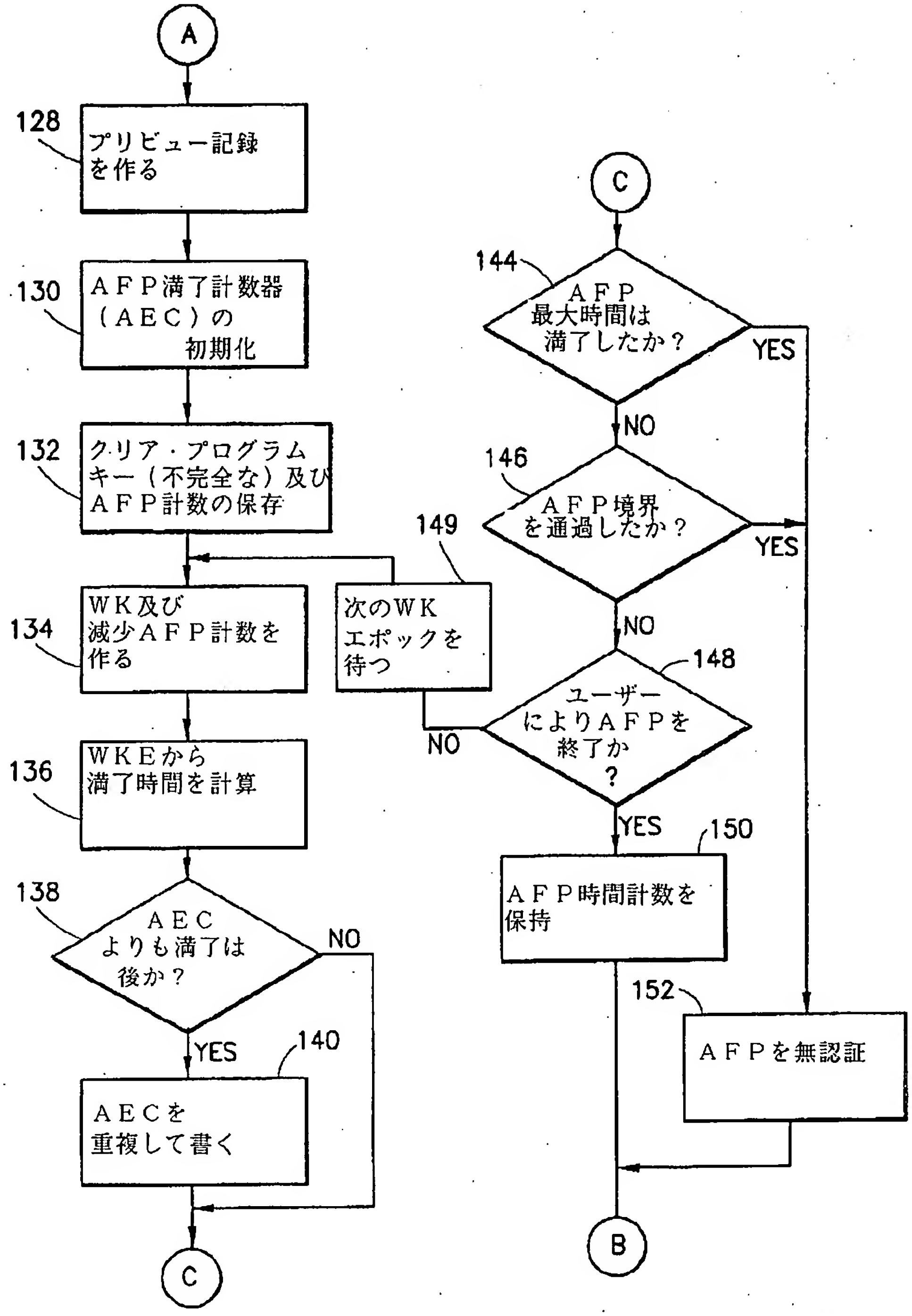
[Drawing 5]


記 録 1
記 録 2
記 録 3
記 録 4
記 録 N
90
92
94
96
98
プログラム属性
プリビュー記録
フリーWK計数
購入記録
番組がプリビューされていると、変更できない
記録有効フラッグ
購入フラッグ
満了タイマー
番組識別器

[Drawing 6]


開始
100
102
WKEメッセージを得る
104
プログラム・プリ・キーを得る
106
認証状態を計算
108
番組を購入したか？
YES
NO
110
購入記録を作る
112
クリア・プログラムキー（不完全な）
114
WKを駆動
116
番組エポックは終了したか？
NO
YES
118
購入記録を消去
120
終了
122
番組エポックは終了したか？
YES
NO
124
AFPは入手可能か？
NO
YES
126
AFPを要求したか？
NO
YES
B
A

[Drawing 7]


A
128
プリビュー記録を作る
130
ＡＦＰ満了計数器（ＡＥＣ）の初期化
132
クリア・プログラムキー（不完全な）及びＡＦＰ計数の保存
149
次のＷＫエポックを待つ
134
ＷＫ及び減少ＡＦＰ計数を作る
136
ＷＫＥから満了時間を計算
138
ＡＥＣよりも満了は後か？
NO
YES
140
ＡＥＣを重複して書く
C
C
144
ＡＦＰ最大時間は満了したか？
YES
NO
146
ＡＦＰ境界を通過したか？
YES
NO
148
ユーザーによりＡＦＰを終了か？
NO
YES
150
ＡＦＰ時間計数を保持
152
ＡＦＰを無認証
B

-- [Written Amendment]

[Filing Date] Heisei 8(1996) March 15

[Amendment 1]

[Document to be Amended] Description

[Item(s) to be Amended] Claims
[Method of Amendment] Change
[Proposed Amendment]
[Claim(s)]
[Claim 1] It is a method for providing video service to a consumer through an information network,
The process which provides meter-rate based video service in program epoch,
The process which forms fixed time in said program epoch when said a part of video service can be seen beforehand,
The process which shows a consumer said a part of video service without purchase beforehand rather than said fixed time always before the short-time maximum preview epoch time and during said fixed time,
How to consist of the process which strengthens said maximum preview epoch time by the security method by encryption.
[Claim 2] It is a method according to claim 1,
How to consist of the process at which a consumer can purchase said video service for seeing in said program epoch after showing the part beforehand further.
[Claim 3] It is a method according to claim 1 or 2,
Said program epoch is divided into two or more working key epoch (WKE),
The process which attests said calculation of WKE by encryption,
How to use this attested calculation and consist of the process which gives said maximum preview time further.
[Claim 4] It is a method given in either of 3 from Claim 1,
It consists of the process holding the record which can direct the amount of the intact preview time which remains to said consumer who looks at said video service during said fixed time further,
The method that said record is held by the security method by encryption.
[Claim 5] It is a method given in either of 4 from Claim 1,
The process holding record of the service which said consumer has seen beforehand in former program epoch,
How to consist of the process which forbids said consumer from looking at service beforehand into the present program epoch when said consumer has seen all the portions of this service beforehand in former program epoch further.
[Claim 6] It is a method according to claim 5,
The method that said record of service is held by the security method by encryption
[Claim 7] It is a method given in either of 6 from Claim 1,
It is a process holding the AKUCHIBU record to N of the service which can be previewed at a

certain time. The process which consists of either the record of purchase as which each of this record expresses the service which was purchased by said consumer, and which can be previewed, or the preview record as which said consumer expresses the service chosen between previews,
How to consist of the process which does not make the service record in which an AKUCHIBU preview is possible complete further until the program epoch for the service expressed by the record is completed.
[Claim 8] It is a method according to claim 7,
How to consist of the process which does not eliminate any preview records further until the service expressed by it is completed.
[Claim 9] It is a method according to claim 7,
The process which changes preview record into record of purchase by purchase by the consumer of service to whom it is expressed by this preview record,
How to consist of the process prevented from changing the record of purchase acquired from said process to change further.
[Claim 10] It is a method according to claim 9,
How to consist of the process which does not eliminate any preview records further until the program epoch for the service expressed by it is completed except for being based on conversion to the record of purchase which cannot be changed.
[Claim 11] It is a method given in either of 10 from Claim 7,
It is the method of consisting of the process which refuses any previews to said consumer further always, when all the service records that can preview N pieces are AKUCHIBU.
[Claim 12] It is a method given in either of 11 from Claim 1,
The way the amount of intact preview time includes further the process which tells said consumer about which remains in said video service.
[Claim 13] It is a method given in either of 12 from Claim 7,
The method that said fixed time is strengthened with the security method by encryption.
[Claim 14] It is equipment for offering the preview of the service which can be purchased through a communication network,
It is the 1st means for processing the data which receives from said communication network. said data identifies the service in which (1) purchase is possible -- (2) -- [the epoch for which said service is provided / identify and] (3) 1st means to offer information required to generate a key to be able to indicate whether a preview is available with said service, and for the consumer by whom (4) permissions were done receive said service or its preview,
2nd means to hold the truck of fixed time between said epoch if what it is 2nd means to answer said 1st means, and is seen beforehand is permitted when a preview is available with said service,

They are said 1st and 2nd means and the user interface which **** so that a consumer can see said a part of service beforehand before the short-time maximum preview time and during said fixed time rather than said fixed time at any time. The user interface with which a consumer can also purchase said service with said user interface,
Equipment which consists of a means to answer said 1st means for decoding said service, during a preview and after the purchase.
[Claim 15] It is equipment according to claim 14,
Equipment which consists of the means for strengthening said maximum preview time with the security method by encryption further.
[Claim 16] It is equipment given in Claim 14 or either of 15,
Equipment which consists of the means for holding record by the security method by encryption further in order to direct the amount of the intact preview time left behind to said consumer who can see said service during said fixed time.
[Claim 17] It is equipment given in either of 16 from Claim 14,
It is a means for holding record to N of the service in which an AKUCHIBU preview is possible at a certain time. The means which consists of either showing the service chosen for the preview of the record of purchase as which each of this record expresses the service which was purchased by said consumer, and which can be previewed, or said consumer of the preview records,
Equipment which consists of the means for not making the service record in which an AKUCHIBU preview is possible complete further until the program epoch for the service expressed by the record is completed.
[Claim 18] It is equipment according to claim 17,
Equipment which consists of the means for not eliminating any preview records further until the program epoch for the service expressed by it is completed.
[Claim 19] It is equipment according to claim 17,
The means for changing preview record into record of purchase by purchase by the consumer of service to whom it is expressed by this preview record,
Equipment which consists of the means for the ability not to change the record of purchase offered by the means for [said] changing further.
[Claim 20] It is equipment according to claim 19,
Equipment which consists of the means for not eliminating any preview records further until the program epoch for the service expressed by it is completed except for being based on conversion to the record of purchase which cannot be changed.
[Claim 21] It is equipment given in either of 20 from Claim 17,
It is equipment which consists of the means for also refusing the service in which what kind of additional preview or additional preview is possible to said consumer always when all the

service records that can preview N pieces are AKUCHIBU further.
[Claim 22] It is equipment given in Claim 14 or either of 21,
Equipment which consists of the means for telling said consumer about the amount of the intact preview time which remains with said service further.
[Claim 23] It is equipment given in Claim 14 or either of 22,
Equipment which said epoch is divided into two or more working key epoch, and is used in order that the calculation attested by the encryption may give said maximum preview time.
[Claim 24] It is equipment given in Claim 14 or either of 23,
Equipment with which a preview consists of a means for attesting the portion of said data by encryption at least to identify whether it is available, further with said service.
[Claim 25] It is equipment given in Claim 14 or either of 24,
Equipment with which said fixed time is strengthened with the security method by encryption.

[Translation done.]